UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

| | |
|---|---|
| INTERSTATE REMOVAL, LLC,<br>Plaintiff,<br>v.<br>NATIONAL SPECIALTY INSURANCE COMPANY,<br>Defendant. | Case No. 23-CV-0510 (PJS/DLM)<br>ORDER |

J. Vincent Stevens, MILLER & STEVENS, P.A., for plaintiff.

Gabriel E. Darwick, COUGHLIN MIDLIGE & GARLAND LLP, for defendant.

Plaintiff Interstate Removal, LLC ("Interstate") lost hundreds of thousands of dollars as a result of two wire transfers that were made from Interstate's bank account to the bank account of a fraudster. The first wire transfer resulted from the fraudster tricking an Interstate employee; the second resulted from the fraudster tricking Interstate's bank. Interstate's insurer, defendant National Specialty Insurance Company ("National"), covered the losses caused by the second transfer but not those caused by the first. Interstate filed this action seeking indemnification for the losses caused by the first transfer.

This matter is before the Court on National's motion to dismiss Interstate's amended complaint. For the reasons that follow, National's motion is granted, and Interstate's amended complaint is dismissed with prejudice.

## I. BACKGROUND

Interstate provides snow removal and other services for commercial properties. Am. Compl. ¶ 16, ECF No. 7. As part of its business, Interstate regularly purchases vehicles from Ryder Vehicle Sales, LLC ("Ryder"). Am. Compl. ¶ 17.

In May 2022, Interstate employee Jim Allen received an email from Ryder requesting payment for vehicles that Interstate had recently purchased. Am. Compl. ¶ 19. Consistent with Interstate's normal practice, Allen forwarded the email to Jill Barger, the Interstate employee responsible for paying outstanding invoices. Am. Compl. ¶ 20. As she had always done when transacting with Ryder, Barger emailed Ryder and asked for wire-transfer information so that she could process the payment. Am. Compl. ¶ 21. Ryder responded with the wire-transfer information, a bill of sales, and a wire-transfer form. Am. Compl. ¶ 22. In total, Interstate agreed to send Ryder two payments of $178,936.93 each. Am. Compl. ¶ 24. A couple of days later, Ryder contacted Barger to inquire about the wire transfer, and Barger told Ryder that she would initiate the first transfer the following morning. Am. Compl. ¶¶ 25–26.

So far, so good. At this point, however, a fraudster "hacked into Interstate's email system and saw the correspondence and imminent wire transfers between the two businesses and took advantage." Am. Compl. ¶ 29. The fraudster sent an email to Barger using the same Ryder email address (and a nearly identical signature block) telling Barger to send the payment to Ryder's "updated bank account." Am. Compl. ¶¶ 28–30. Barger responded, asking for the updated account information, and the fraudster replied with a new bank-account number and a revised wire-transfer form. Am. Compl. ¶¶ 31–32. Barger initiated the wire-transfer process with Interstate's bank, which verified the transfer request through another Interstate employee and then wired $178,936.93 from Interstate's account to the fraudster's. Am. Compl. ¶¶ 34–35.

Nearly a week later, the fraudster (this time impersonating Barger and using her email address) sent an email directly to Interstate's bank, instructing the bank to make the second wire transfer of $178,936.93 to the fraudster's account. Am. Compl. ¶ 37. Only then did Interstate realize that it had been defrauded. Am. Compl. ¶ 38. Interstate contacted its bank and law enforcement, but the bank had already made the second transfer, and the fraudster had disappeared with the money. Am. Compl. ¶ 37.

Interstate then sought indemnification from National, which insured Interstate under Commercial Cyber Insurance Policy Number BLU-CV-M5C5QQV3X-002. Am. Compl. ¶¶ 6, 39; Am. Compl. Ex. A, ECF No. 27 ("Policy"). After investigating

Interstate's claim, National agreed to cover the losses that Interstate suffered as a result of the second transfer (which losses were caused by the fraudster impersonating Barger to Interstate's bank), but not for the losses suffered as a result of the first transfer (which losses were caused by the fraudster impersonating Ryder to Barger). In this lawsuit, Interstate seeks coverage for the first transfer under two endorsements to the Policy: (1) the Computer and Funds Transfer Fraud Endorsement and (2) the Social Engineering Endorsement. Am. Compl. ¶¶ 6–7.

## II. ANALYSIS

### *A. Standard of Review*

In reviewing a motion to dismiss for failure to state a claim under Fed. R. Civ. P. 12(b)(6), a court must accept as true all of the factual allegations in the complaint and draw all reasonable inferences in the plaintiff's favor. *Perez v. Does 1–10*, 931 F.3d 641, 646 (8th Cir. 2019). Although the factual allegations need not be detailed, they must be sufficient to "raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). The complaint must "state a claim to relief that is plausible on its face." *Id.* at 570.

### *B. Coverage*

The parties agree that their coverage dispute is governed by Minnesota law, under which an "insurance policy must be construed as a whole, and unambiguous language must be given its plain and ordinary meaning." *Midwest Fam. Mut. Ins. Co. v. Wolters*, 831 N.W.2d 628, 636 (Minn. 2013) (quotation omitted). "Language in a policy is ambiguous if it is susceptible to two or more reasonable interpretations." *Id.* (citation omitted). Ambiguous terms are construed in favor of coverage, but courts must "not read an ambiguity into the plain language of a policy in order to provide coverage." *Eng'g & Constr. Innovations, Inc. v. L.H. Bolduc Co.*, 825 N.W.2d 695, 705 (Minn. 2013) (quotation omitted).

As noted, Interstate seeks coverage under both the Computer and Funds Transfer Fraud Endorsement and the Social Engineering Endorsement. The Court will address each endorsement in turn.

### 1. Computer and Funds Transfer Fraud Endorsement

Section A of the Computer and Funds Transfer Fraud Endorsement provides coverage as follows:

> 1. We will pay for:
>
> a. Loss resulting directly from a fraudulent:
>
> (1) Entry of Electronic Data or Computer System[1] into; or
>
> (2) Change of Electronic Data or Computer System within;

[1] Neither party disputes that the fraud alleged implicates "Electronic Data" and "Computer System," as those terms are defined in the Policy.

> a Computer System, provided the fraudulent entry or fraudulent change causes, with regard to Paragraphs 1.a.(1) and 1.a.(2):
>
> (a) Money, securities or other property to be transferred, paid or delivered; or
>
> (b) Your account at a financial institution to be debited or deleted.

Policy 33.[2]

Section C of the Endorsement contains the following exclusion:

> 1. We will not be liable for Loss resulting from: . . .
>
> d. An Employee or financial institution acting upon any instruction to:
>
> (1) Transfer, pay or deliver money, securities or other property; or
>
> (2) Debit or delete your account;
>
> which instruction proves to be fraudulent . . . .

Policy 35.

[2] Because the exhibit contains non-consecutive pagination and sectioning, the Court cites to the page numbers generated by the Court's CM/ECF filing system.

The parties first dispute whether Interstate's loss is covered by the insuring grant found in Section A.1.a of the Computer and Funds Transfer Fraud Endorsement.[3] National argues that Interstate's loss did not "result[] directly" from a fraudulent entry or change of electronic data, as required under Section A.1.a, because it was Barger's request to the bank, and not the fraudster's hack of Interstate's computer system, that caused the loss. National relies on *SJ Computers, LLC v. Travelers Cas. & Ins. Co. of Am.*, 621 F. Supp. 3d 962, 967–70 (D. Minn. 2022), in which this Court found that a similar fraud scheme was not covered under a similar computer-fraud policy.

National's reliance on *SJ Computers* is misplaced, however. The policy in *SJ Computers* covered both computer fraud and social-engineering fraud and made clear that, for purposes of the policy, they were "mutually exclusive categories." *Id.* at 968. The Court held that it was absolutely clear that the loss that SJ Computers had suffered was the result of social-engineering fraud: "[T]he drafters of the Policy anticipated precisely the type of fraud that victimized SJ Computers, defined that fraud as social-

[3] Interstate also seeks coverage under Section A.1.b, which covers loss from a "Fraudulent Instruction directing a financial institution to debit your Transfer Account and transfer, pay, or deliver money or securities from the account." Policy 33. Under the Policy, however, "Fraudulent Instruction" is defined to include only instructions that purport to come from the insured or an employee of the insured, but that in fact come from someone else without the insured's knowledge or consent. Policy 34. This is what happened with respect to the second transfer. With respect to the first transfer, however, Interstate's pleadings are clear that the instruction directing Interstate's bank to debit its account came from Interstate, not the fraudster.

engineering fraud, and, for good measure, excluded that fraud from the definition of computer fraud." *Id.* at 969.

That should have been the end of the analysis. But because the limits that applied to computer fraud were higher than the limits that applied to social-engineering fraud, the insured tried to trigger computer-fraud coverage by artificially isolating one *step* in the fraud (the fraudster's use of an employee's email account to forward fraudulent invoices to the company's CEO) and argue that that particular *step* constituted computer fraud. *See id.* The Court responded that the fraud could not be artificially fragmented in that way—and then pointed out that, even if it could, the insured would not be covered:

> If that aspect of the fraudulent scheme is going to be viewed in isolation, then that aspect needs to be viewed in isolation for all purposes.
>
> The bad actor's use of the purchasing manager's email account to forward the fraudulent invoices to the CEO—*when viewed in isolation*—did not "directly cause[ ]" a "direct loss" to SJ Computers. . . . SJ Computers did not suffer a penny of financial loss when the bad actor hit "send" on his email messages. And SJ Computers would never have suffered a penny of financial loss if the CEO had not opened those email messages, or if the CEO had asked the purchasing manager about them, or if ERI Direct had answered its phone when the CEO called, or if ERI Direct had promptly returned the voice-mail message left by the CEO, or if the CEO had waited to hear from ERI Direct before paying the invoices. If the fraudulent scheme that victimized SJ Computers is going to be fragmented into

> pieces and each piece *viewed in isolation*, then what "directly caused" loss to SJ Computers was not the piece involving the bad actor's use of the purchasing manager's account to send the fake invoices, but rather the piece involving the CEO's use of his computer to act on the fake invoices. . . .

*Id.* (emphasis added).

National focuses on this discussion, but ignores the fact that *SJ Computers* held that the fraud could *not* be broken into pieces and each viewed in isolation as the insured proposed. The language relied on by National was just an aside—a comment that, "even if the Court was willing to play this game, you'd still lose." But the Court was not willing to play the game.

And the Court is not willing to play the game in this case by artificially fragmenting the fraud into pieces and focusing on each piece in isolation. Here, unlike in *SJ Computers*, the Court is not confronted with a policy that defines social engineering and computer fraud to be mutually exclusive, nor a policy that "bends over backwards to make clear that this situation involves social-engineering fraud, not computer fraud." *Id.* at 969. Rather, Interstate has alleged that it is entitled to coverage under two separate endorsements to the Policy that define what they cover without reference to each other. Each endorsement can simply be interpreted on its own terms. And as to the meaning of the phrase "resulting directly from," the Court agrees with the cases cited by Interstate that hold that a reasonable insured would understand the phrase "resulting directly from" "to convey the concept of proximate cause." *City of Unalaska v. Nat'l Union Fire Ins. Co.*, 591 F. Supp. 3d 440, 451 (D. Alaska 2022); *see also, e.g.*, *Principle Sols. Grp., LLC v. Ironshore Indem., Inc.*, 944 F.3d 886, 891 (11th Cir. 2019) ("[T]he ordinary meaning of the phrase 'resulting directly from' requires proximate causation between a covered event and a loss, not an 'immediate' link."); *cf. Lipshultz v. Gen. Ins. Co. of Am.*, 96 N.W.2d 880, 885 (Minn. 1959) (finding that loss was a "direct loss by windstorm" within meaning of insurance policy where "the chain of events culminating in the loss . . . was set in motion by a windstorm").

The loss that Interstate suffered as a result of the first transfer was proximately caused by a fraudulent entry of data into Interstate's computer system that resulted in money being transferred from Interstate's bank account. Interstate's loss is therefore covered under Section A.1.a.

That is not the end of the matter, however. Although the Court has held that Interstate's loss falls within the coverage grant found in Section A.1.a, that coverage grant is limited by the exclusion found in Section C.1.d. And unfortunately for Interstate, that exclusion eliminates coverage for its claim. The exclusion provides that National "will not be liable for Loss resulting from . . . [a]n Employee or financial institution acting upon any instruction to [t]ransfer, pay or deliver money, securities or other property . . . which instruction proves to be fraudulent . . . ." Policy 35. As

Interstate itself concedes, this provision plainly bars coverage for losses caused by the first transfer. That *is* the end of the matter.

Interstate argues otherwise, contending that the policy is ambiguous because the exclusion found in Section C.1.d wipes out all of the coverage provided in Section A.1.b. Section A.1.b covers loss from a "Fraudulent Instruction directing a financial institution to debit your Transfer Account and transfer, pay, or deliver money or securities from the account." Policy 33. According to Interstate, there is a conflict between Section A.1.b. and Section C.1.d., and that conflict renders either Section A.1.b or Section C.1.d (or both) ambiguous, making it improper to dismiss the amended complaint under Rule 12(b)(6). *Cf. Rusthoven v. Com. Standard Ins. Co.*, 387 N.W.2d 642, 644–45 (Minn. 1986) ("Since [two applicable endorsements] are irreconcilably inconsistent, the policy is ambiguous and, therefore, is to be strictly interpreted against the insurer.").

The Court disagrees. To begin with, any conflict between Sections A.1.b and C.1.d is irrelevant, as Section A.1.**b** affords no coverage for Interstate's loss. As explained above, Section A.1.**a** does afford coverage, and then Section C.1.d is unambiguous in excluding from that coverage losses such as Interstate's. Section C.1.d does not, however, wipe out *all* of the coverage provided by Section A.1.a. For example, suppose that a fraudster hacked into Interstate's computer system and, posing as an Interstate employee, sent an email to Ryder instructing Ryder to deliver vehicles that

Interstate had purchased to a location chosen by the fraudster. The loss of the vehicles would seem to be covered by Section A.1.a: Interstate would have suffered a loss resulting directly from the entry of data into its computer system that caused property to be transferred to the fraudster. Section C.1.d would not eliminate that coverage as no financial institution would be involved.

It may be true that Section C.1.d eliminates *most* of the coverage provided by Section A.1.a. That does not make policy ambiguous, however, but just less useful to Interstate. The Court therefore must decline Interstate's invitation to "read an ambiguity into the plain language of a policy in order to provide coverage." *Eng'g & Constr. Innovations,* 825 N.W.2d at 705 (quotation omitted). The Court holds that there is no coverage under the Computer and Funds Transfer Fraud Endorsement for the losses suffered by Interstate as a result of the first transfer.

### 2. Social Engineering Endorsement

The Social Engineering Endorsement provides coverage for a "Social Engineering Loss resulting directly from a Social Engineering Incident," which, roughly speaking, refers to the insured transferring money to a fraudster in good-faith reliance on a fraudulent email instruction. The provision also imposes a condition precedent: "As a condition precedent to coverage, the Insured's established and documented verification procedure must have been followed before acting upon such instruction." Policy 37.

Section II of the Social Engineering Endorsement then sets forth the following exclusion:

> We will not be liable for Social Engineering Loss resulting from a Social Engineering Incident based upon, attributable to or arising out of: . . .
>
> 6. Money or other property being transferred, paid or delivered as a result of Security Breach or Cyber Incident.

Policy 38. The general Policy defines a "Cyber Incident" to include, in relevant part, a "Hacker attack . . . that is directed at, enacted upon or introduced into a Computer System . . . and is designed to access, alter, corrupt, damage, delete, destroy, disrupt, encrypt, use or prevent or restrict access to or the use of any part of a Computer System . . . ." Policy 18. A "Hacker," meanwhile, is defined in the Policy essentially as a person who accesses a computer system without authorization. Policy 20.

National argues that the Social Engineering Endorsement does not cover Interstate's loss for two reasons. First, National argues that Interstate failed to meet the condition precedent to coverage. Second, National argues that Interstate's loss falls within the Section II.6 Exclusion. The Court agrees with both of National's arguments.

### *a. Condition Precedent*

National contends that there is no coverage under the Social Engineering Endorsement because Interstate has failed to allege compliance with the condition precedent to coverage, which requires Interstate to follow an "established and documented verification procedure . . . before acting upon" a fraudulent instruction to transfer money. Policy 37. Under Minnesota law, conditions precedent "must be literally met or exactly fulfilled, or no liability can arise on the promise qualified by the condition." *Capistrant v. Lifetouch Nat'l Sch. Studios, Inc.*, 916 N.W.2d 23, 27–28 (Minn. 2018) (quotation omitted).

Interstate argues that it has pleaded compliance with the condition precedent by alleging that (1) Allen forwarded the initial payment request from Ryder to Barger, as he normally did; (2) Barger responded to Ryder by asking for wire-transfer information, as she normally did; and (3) the bank verified Barger's transfer request with another Interstate employee, as it normally did. Drawing all reasonable inferences in Interstate's favor, the Court agrees that Interstate has sufficiently alleged that it followed a procedure when acting on Ryder's initial (authentic) wire-transfer instruction, and that the procedure was established. But Interstate must allege more—not only that it followed an *established* procedure, but that it followed a *documented* procedure when it responded to the fraudster's email. Policy 37.

The allegations in Interstate's amended complaint fall short for three reasons:

First, no where does the amended complaint allege that the procedure that Interstate followed was both "established *and documented*." Interstate has merely alleged that it had an (undocumented) practice of processing payment requests from Ryder in a particular way, and that Allen and Barger followed that usual practice.

Interstate argues that its procedure was "documented" in the sense that its interactions with Ryder and the fraudster were captured in email records. This is a creative way of interpreting the Policy's language, but not a reasonable one. The policy does not require that each step taken pursuant to the procedure have been "established and documented"; it requires that *the verification procedure itself* must have been "established and documented"—such that an insurer could walk into Interstate, ask to see the verification procedure, and be handed a document. What would it even mean to say that, say, an email from Barger to Ryder was "established"?

Second, there is no way to construe the steps that Interstate allegedly took as a *verification* procedure—that is, a procedure "to establish the truth, accuracy, or reality of" the wire-transfer requests.[4] Interstate sought information from Ryder—both the real Ryder and the fraudster-posing-as-Ryder—but did nothing to verify that the information it received in response was true.[5]

[4] *Verify*, Merriam-Webster, https://www.merriam-webster.com/dictionary/verify (last visited February 28, 2024).

[5] Interstate also cannot piggyback on the *bank's* process for verifying that it was receiving an authentic wire-transfer request *from Interstate*. The Policy requires *Interstate* (not its bank) to follow the requisite verification procedure. Moreover, the Policy requires Interstate to do so "before acting upon" an imposter's instruction.

(continued...)

Third, the Policy requires not only that the insured have an "established and documented" verification procedure, but that the insured *follow* that procedure before acting on an instruction coming from an imposter. See Policy 37 (defining "Social Engineering Incident" as action taken in reliance on email instruction "which contained a fraudulent and material misrepresentation and was sent by an imposter"). Interstate points to various things it did in response to Ryder's initial (genuine) wire-transfer request, but Interstate has not pointed to *anything* it did in response to the fraudster's instruction (beyond asking the fraudster for the updated banking information). To the contrary, the amended complaint makes clear that Barger did nothing to verify that Ryder in fact had an updated bank account and that the account information received from the fraudster was in fact tied to an account owned by Ryder. She simply accepted the fraudster's instructions at face value.

In sum, because Interstate has failed to allege that it complied with a condition precedent to coverage under the Social Engineering Endorsement—specifically, that it followed an "established and documented verification procedure . . . before acting upon" the fraudster's instruction—the Social Engineering Endorsement provides no coverage for the losses suffered by Interstate as a result of the first transfer.

[5](...continued)
Policy 37. Interstate had already acted upon the fraudster's instruction by the time the bank took its verification steps.

### *b. Section II.6 Exclusion*

Even if Interstate had pleaded that it complied with the condition precedent, coverage would still be barred by the exclusion found in Section II.6 of the Social Engineering Endorsement. That exclusion provides, in relevant part, that National will not be liable for social-engineering loss arising out of "[m]oney or other property being transferred, paid or delivered as a result of . . . [a] Cyber Incident." Policy 38. "Cyber Incident" is defined elsewhere in the Policy as encompassing any "Hacker attack . . . designed to access . . . [or] use . . . any part of a Computer System." Policy 18.

Here, undoubtedly in an effort to take advantage of the higher coverage limits that apply to the Computer and Funds Transfer Fraud Endorsement, Interstate has alleged that the fraudster "hacked into Interstate's email system and saw the correspondence and imminent wire transfers between the two businesses and took advantage" and that "[t]he Fraudster entered the Interstate email system and changed the wire transfer information within the system and then sent that updated, but wrong, information to Ms. Barger." Am. Compl. ¶¶ 29, 33. In other words, Interstate has alleged that its loss stemmed from the fraudster's unauthorized access into and use of Interstate's email system, thus pleading its way directly into the Section II.6 exclusion.

In its brief, however, Interstate attempts to backpedal, now asserting that "nobody really knows" how the fraudster learned about the imminent wire transfers or inserted himself into the conversation. Plf.'s Mem. Opp'n 34, ECF No. 34. But Interstate's amended complaint pleads—over and over again—that the fraudster hacked into Interstate's email system. Interstate could have pleaded something else in the alternative, but it did not, and Interstate cannot now use a brief to amend its complaint. *See Fischer v. Minneapolis Pub. Schs.*, 792 F.3d 985, 990 n.4 (8th Cir. 2015).[6]

For these reasons, the Court finds that National is not required to indemnify Interstate for the losses it suffered as a result of the first transfer under either the Computer and Funds Transfer Fraud Endorsement or the Social Engineering Endorsement. Interstate's amended complaint is therefore dismissed.

ORDER

Based on the foregoing, and on all of the files, records, and proceedings herein, IT IS HEREBY ORDERED THAT defendant's motion to dismiss [ECF No. 28] is GRANTED. Plaintiff's amended complaint [ECF No. 7] is DISMISSED WITH PREJUDICE AND ON THE MERITS.

LET JUDGMENT BE ENTERED ACCORDINGLY.

[6] Interstate asks for leave to amend its complaint a second time so that it can plead that nobody knows the details about how the fraudster executed his crime. But Interstate's proposed amendment would be futile, as it would not overcome the fact that Interstate cannot plead compliance with the condition precedent.

Dated: March 28, 2024

s/Patrick J. Schiltz
Patrick J. Schiltz, Chief Judge
United States District Court